Making Your Django App GDPR Compliant

By Sushil Kambampati

What is GDPR

- European Union's General Data Protection Regulation - comprehensive set of rules that attempt to protect individual's privacy and give them control over information about themselves
- Affects Data Controllers and Processors based in the EU and those outside the EU that collect or process information of EU residents
- GDPR has teeth: top fine of up to €20 million or 4% of prior turnover, whichever is greater

Why Should You Care?

- You may have users in the EU
- You may one day want to have users in the EU
- You may want your company to be acquired by a company that is based in the EU
- You may want your company to be acquired by a company that has users in the EU
- You may want your company to go public

Protections and Rights

- Informed consent
- Consent must be explicit
- Consent may be withdrawn
- Right of access to collected data
- Right to port collected data
- Right to rectify collected data
- Right to be forgotten
- The pseudonymisation of personal data

Informed Consent

- "concise, easily accessible and easy to understand, and that clear and plain language"

Consent must be explicit

- The user must take an action to grant consent.
- Pre-ticked check-boxes are a no-no

Consent may be withdrawn

- The user may at any point withdraw consent
- Make sure it has real effect

Right of access to collected data

- A user may request access to the data collected by the app.
- Machine Learning systems may pose a challenge here

Right to port collected data

- GDPR envisions users porting their data from one collector to another
- Could have application in health systems, job sites or video streaming, as examples.

Right to rectify collected data

- People have the right to correct information about themselves

Right to erasure

- Individuals may request that information about them be erased
- May not be possible in many cases − financial transactions
- However, personally identifiable information may be removed or overwritten

The pseudonymisation of personal data

- What is pseudonymization
- Potential approaches
- Circumstances dependent
- Practicable options